Accellion Share Securely™

AN ACCELLION WHITE PAPER

Mitigating the Security Risks of File Sharing and Collaboration in the Enterprise

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

Executive Summary

Stories about data breaches continue to make the headlines every week, and yet enterprises continue to rely on email, IM, FTP, USB flash drives, and CDs for transferring files. The WikiLeaks data breach of U.S. diplomatic cables reminds us that even the most sensitive and what should be heavily guarded data can be leaked through file sharing technology as commonplace as a CD/RW drive.

When enterprises lose control of files with confidential or sensitive information, dire consequences ensue. Competitors discover intellectual property and strategic plans. Criminals steal identities and siphon funds. Customers defect to competitors. There are also strict penalties associated with infractions of regulations such as GLBA, HIPAA, and SOX.

To prevent these data breaches, enterprises should first conduct a thorough audit of their file sharing practices. Is your organization still relying on FTP or USB flash drives? Are you monitoring email and IM? Have you disabled the CD drives on employees' laptops?

Once an enterprise has audited its file sharing technologies, it should control or discontinue use of risky technologies. In their place, organizations should deploy a secure file transfer solution that makes it easy for employees to share files securely with internal and external parties. The secure file transfer solution should enforce fine-grained security policies and provide audit and reporting features for IT managers, compliance officers, and other members of the IT security team.

Implementing a secure file sharing solution minimizes the risk of data breaches and helps ensure compliance with internal policies and industry regulations.

Introduction

Is anyone in your organization still using CDs, FTP, or USB sticks to transfer Protected Health Information (PHI)? If so, your organization is at risk for non-compliance with the Health Insurance Portability and Accountability Act (HIPAA). Your organization is also running the risk of a serious data breach, making news headlines, and incurring hefty regulatory fines.

As a cautionary tale, consider the case of a doctor at NYU Langone Medical Center who used an unencrypted USB stick to store the PHI of 2,563 patients undergoing procedures at the clinic. The data included names, ages, genders, medical record numbers, and descriptions of medical procedures. When the USB stick was discovered missing in May 2010, the medical center was forced to notify patients and the public of its data breach.[1] Many organizations that disclose breaches like this soon find themselves the subjects of civil lawsuits.

The Office of Civil Rights fined Rite Aid $1 million for disposing prescription information in trashcans outside of Rite Aid stores.

NYU got off pretty lightly, all considered. The pharmaceutical giant Rite Aid is paying a steeper price for its own PHI security breach. Rite Aid employees were caught disposing of prescription information in trash cans outside Rite Aid stores. The Office of Civil Rights (OCR) in the Department of Health and Human Services (HHS) concluded that this behavior violated HIPAA regulations. For this indiscretion, the OCR fined Rite Aid $1 million.[2]

PHI data breaches are all too common. In the past year alone, the HHS was notified of 166 major data breaches, each affecting at least 500 patients, and affecting 4.9 million PHI data sets in total.[3] Nearly a quarter of healthcare organization CIOs reported suffering a security breach in the previous 12 months.[4] Some of these breaches involved USB sticks or stolen laptops. Others involved careless email messages or unprotected servers. All of them put healthcare organizations (HCOs) at risk of financial penalties, tarnished brands, and lost business.

Everyday Dangers

File sharing is essential to business. It would be nearly impossible to design a product, offer a service, close a transaction, or perform countless other tasks without sharing files. Many of these files are confidential. Keeping them confidential requires that employees share them in a secure, auditable way.

Unfortunately, the file sharing technologies employees use every day may not be as secure as you think. Consider the following data breaches:

- The spouse of a Pfizer employee installed P2P software on a company laptop, presumably to share music or movie files. The software inadvertently leaked confidential personnel files onto the Internet. The leaked data included names,

[1] http://www.phiprivacy.net/?p=3108
[2] http://www.hhs.gov/news/press/2010pres/07/20100727a.html
[3] http://www.docehrtalk.org/messageboard/2010/10/01/hhs-presents-major-data-breaches-line
[4] The 2010 HIMSS (Healthcare Information and Management Systems Society) Leadership Survey, http://www.himss.org/2010Survey/

addresses, Social Security numbers, and salary information for current and past employees of the company.[5]

- A reporter for *InformationWeek* was able to search for confidential information and discover detailed medical records, credit reports, the fund-raising plan of a state political party, cell phone numbers for senators, and more by using a search feature in LimeWire, a P2P application supposedly installed on nearly 20% of all computers.[6]
- A lost, unencrypted USB flash drive contained information about staff transfers at a nuclear power plant and inspections by the International Atomic Energy Agency.[7]
- In Mesa County, Colorado, 20 years' worth of internal law enforcement records were left on an unsecure FTP server and made accessible to the public. In another FTP breach, a computer with an IP address in Iran downloaded data about critical city infrastructure in Greensboro, North Carolina.[8]

Unfortunately, the file sharing technologies employees use every day may not be as secure as you think.

And let's not forget the biggest data breach of 2010: U.S. Army Specialist Bradley Manning used a CD/RW drive to copy video footage and hundreds of thousands of diplomatic cables from a supposedly secure communications room. He gave this data to the organization WikiLeaks, which released much of the data to news organizations and its own network of websites.[9] The disclosure of this confidential information had diplomats and governments around the globe scrambling to shore-up alliances and to downplay incriminating information. The full effects of this disclosure will probably not be understood for many years.

There are also strict penalties associated with regulatory infractions, including violations of:

- Sarbanes-Oxley (SOX), which requires businesses to control the distribution of material information
- Gramm-Leach-Bliley (GLBA), which requires financial services firms to protect confidential customer records
- HIPAA, which requires health care organization and their business partners to protect patient health information (PHI). State and federal privacy laws, such as the Massachusetts Data Privacy Law, which requires businesses to put in place stringent data protection controls and to publically announce data breaches.

[5] "Your Data And The P2P Peril," John Foley, *InformationWeek*, http://www.informationweek.com/story/showArticle.jhtml?articleID=206903416

[6] "Our P2P Investigation Turns Up Business Data Galore," Avi Baumstein, *InformationWeek*, http://www.informationweek.com/story/showArticle.jhtml?articleID=206903417

[7] "Nuclear Station Suffers USB Data Breach," Tom Jowitt, *eWeek UK,* http://www.eweekeurope.co.uk/news/nuclear-station-suffers-data-breach-from-lost-usb-stick-10731

[8] "New policy to prevent data breach," *The Daily Sentinel*, http://www.gjsentinel.com/news/articles/new_policy_to_prevent_data_bre

[9] "'I Can't Believe What I'm Confessing to You': The Wikileaks Chats", *Wired Magazine*, Kevin Poulsen and Kim Zetter, http://www.wired.com/threatlevel/2010/06/wikileaks-chat/

Do You Know Where Your Files are Going?

How secure is your organization's file sharing IT infrastructure? Is your organization following best practices for sharing files securely? Or is it still relying on email, CDs, courier services, USB flash drives, and keeping its fingers crossed? Are your employees using free personal email and file sharing accounts such as Yahoo Mail, DropBox, Box.net, and YouSendit, thereby limiting your visibility to potential data breaches?

To assess the security of your organization's file sharing security, ask yourself the following questions.

SECURITY POLICIES AND EMPLOYEE TRAINING

- Has your organization defined and published security policies for sharing files?
- Does your organization forbid the use of P2P software, free webmail and file sharing services, and other risky applications?
- Are security policies and best practices communicated to all employees, including new hires and contractors?
- Do employees know whom to contact if they have questions or concerns about best practices or possible security breaches?

SECURITY MANAGEMENT AND MONITORING

- Does your organization have a way of monitoring the sharing of confidential files?
- Does your organization regularly audit file sharing for security violations?

EMAIL

- Does your organization monitor files sent through email?
- Does your organization block users from sending files, especially large files, to free email addresses, such as addresses at yahoo.com or gmail.com?
- Does your organization require confidential files to be sent encrypted?

IM

- Does your organization monitor the use of IM on its network? Does your organization allow users to transfer files over IM?

Has your organization standardized on an IM client? If so, does the client support encryption of messages and of files?

FTP

- Does your organization monitor file access on FTP servers?

P2P

- Does your organization forbid the installation of P2P applications on its systems? Does your organization monitor network traffic for data leaks from

P2P applications such as Gnutella?

CDS, USB FLASH DRIVES, AND COURIERS

- Does your organization disable the CD drives and USB ports on employee desktops or laptops?
- When confidential information is copied to external media such as CDs, is the data always encrypted?
- Does your organization rely on courier services to deliver confidential files? If so, do you track all files that are delivered this way?

Fixing the Problem of Unsecure File Sharing

To ensure data security and compliance for your organization, you need to know all your data security risks and how to mitigate them. It is important that you implement best practices for secure file sharing, so employees can continue to collaborate with internal and external parties.

Best practices include the following:

1. **DEFINE SECURITY POLICIES AND EDUCATE USERS**
   Define security policies for sharing information via email, IM, and file transfers in general. Educate users about these policies regularly.

2. **PROHIBIT THE USE OF FREE PERSONAL EMAIL AND FILE SHARING ACCOUNTS**
   Forbid the use of free file-sharing services and public webmail accounts. The IT department should be monitoring all methods used for transferring files. Install applications such as Websense for monitoring web traffic and blocking risky sites.

3. **ENSURE IM IS SECURE**
   Warn users about the dangers of communicating over unencrypted IM channels. Require employees to use all the relevant security features of their IM clients.

4. **REPLACE FTP**

   Disable FTP servers and close all unnecessary accounts. Monitor servers to ensure that confidential files are not posted or left unattended on FTP servers.

5. **PREVENT THE USE OF USB FLASH DRIVES AND CDS**
   Disable USB ports on desktop systems and laptops to discourage the use of USB flash drives for backing-up or transferring files. Whenever appropriate, also disable the CD drives. Educate employees about the dangers of unencrypted USB flash drives and CD drives. If users are going to make use of these media, provide them with the necessary security features.

6. **STOP THE P2P THREAT**
   Forbid the use of P2P applications on enterprise systems and networks.

Educate users about the risks of P2P networks and monitor your network for P2P traffic.

7. **PROVISION A SECURE FILE TRANSFER SOLUTION**
   Deploy an easy-to-use file transfer solution enterprise-wide that encrypts files and sends them securely to authorized users. The solution should log every file transfer and file access. It should also provide granular controls for tracking all transfer activity and enabling and disabling accounts. Integrate the solution with email and IM, so that secure file transfer becomes a standard practice for all employees.

8. **STAY VIGILANT TO MEET REGULATORY MANDATES**
   Monitor file sharing activities to ensure that users comply with internal security policies and regulations such as GLBA and HIPAA.

Accellion Secure File Sharing Solutions

Accellion provides enterprise-class secure collaboration and managed file transfer solutions that offer unparalleled flexibility, scalability, and accessibility. Accellion enables organizations to secure and control the sharing of intellectual property and confidential information with internal and external parties for enterprise security and compliance and enhanced business productivity.

KEY BENEFITS OF THE ACCELLION SOLUTION

- Ensures end-to-end file transfer security
- Enables transfer of large files up to 100GB in size
- Enables creation of secure workspaces for sharing and managing files
- Supports threaded discussions about workspaces and files
- Provides comprehensive file tracking for regulatory compliance
- Reduces email storage requirements
- Automates file lifecycle management
- Provides comprehensive reporting capabilities
- Is easy to administer

Accellion Secure File Sharing solutions are used by leading enterprise organizations including Procter & Gamble; Activision; Indiana University Health; Kaiser Permanente; Foley & Mansfield; Lovells; Bridgestone; Ogilvy & Mather; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA.

For more information, please visit www.accellion.com or call +1 650-485-4300.

www.accellion.com **info@accellion.com**

THIS DOCUMENT IS PROVIDED "AS IS." ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.